Number Theory MAS4203 | **Home-A'** | Prof. JLF King 31Aug2015

**Hello.** Essays violate the CHECKLIST at *Grade Peril*!
Exam is due by **11:45AM, Monday, 13Feb2006**.

**A'1:** Show no work.

a $\varphi(169000) =$ _____.
Express your answer a product $p_1^{e_1} \cdot p_2^{e_2} \cdots$ of primes to powers.

b Easily, $\varphi(625) =$ _____. Consequently, $28^{2106} \equiv_{625}$ _____ $\in [0\,..\,625)$. [*Hint:* Fermat, Euler, working mod 625.]

c+ $G := \text{Gcd}(255, 33) =$ _____. A pair $(S, T)$ is ***good*** if both are integers, and $[255 \cdot S] + [33 \cdot T] = G$. Use the LBolt Alg to produce a good pair $S =$ _____, $T =$ _____. Give formulas $S(k) =$ _____ and $T(k) =$ _____ which obtains all good pairs, as $k$ ranges over the integers.

d As polynomials in $\mathbb{Z}_{11}[x]$, let

$$B(x) := 6x^3 - x^2 + x - 2\,;$$
$$C(x) := 3x^2 + 7x - 6\,.$$

Write t.fol polys, using coeffs in [-5 .. 5]. Compute quotient and remainder polynomials
$q(x) =$ _____ & $r(x) =$ _____,
with $B = [q \cdot C] + r$ and $\text{Deg}(r) < \text{Deg}(C)$,

e+ (With $B, C$ from above, polys in $\mathbb{Z}_7[x]$.) Let $D$ be $\text{Gcd}(B, C)$. Using coeffs in [-5 .. 5]: $D(x) =$ _____.
Compute polys $S(x) =$ _____,
$T(x) =$ _____ st. $[S \cdot B] + [T \cdot C] = D$.

**A'2:** Give, with careful proof, a complete list of mod-12 residues $\{$ _____ $\}$, so that 3 is a $p$-QR iff oddprime $p \equiv_{12}$ to some elt of the list. [*Hint:* Use the Jacobi symbol $\left(\frac{3}{p}\right)$ and quadratic reciprocity.]

**A'3:** The number $p := 1217$ is prime. Use the "repeated squaring, mod $p$" technique to compute the Legendre symbols $\left(\frac{5}{p}\right)$ and $\left(\frac{19}{p}\right)$, showing me the steps. Which of $\{5, 19\}$ has a mod-1217 square-root?

**A'4:** Prove, for odd $n \in [3\,..\,\infty)$, that the Jacobi symbol

$$\left(\frac{2}{n}\right) = [-1]^{\frac{n^2-1}{8}}\,.$$

You many use without proof that for an oddprime $p$, the Legendre symbol $\left(\frac{2}{p}\right)$ is +1 if $p \equiv_8 +1$, and $\left(\frac{2}{p}\right) = -1$ otherwise. *Hint:* You may want to prove this Lemma: *For odd posints $r$ and $s$,*

$$\frac{r^2-1}{8} + \frac{s^2-1}{8} \equiv_2 \frac{r^2 s^2 - 1}{8}\,.$$

| | | |
|---|---|---|
| **A'1:** | ___ ___ | 85pts |
| **A'2:** | ___ ___ | 65pts |
| **A'3:** | ___ ___ | 60pts |
| **A'4:** | ___ ___ | 85pts |
| **Total:** | ___ ___ ___ | 295pts |

*Please PRINT your name and ordinal. Ta:*

Ord: _____

HONOR CODE: *"I have neither requested nor received help on this exam other than from my professor."*

Signature: _____